ABSTRACT OF THE DISCLOSURE

A technique for enabling a firewall device to allow encrypted data to securely pass between networks, and at the same time allow the firewall to selectively monitor the encrypted traffic that is allowed to pass is disclosed. In one embodiment, the technique is realized by detecting an exchange of a first encryption key between a host device and a remote device, and the first encryption key supports confidentiality protection of a first security policy between the host device and the remote device. Next, a second encryption key is exchanged with the host device when the exchange of the first encryption key is detected, and the exchange of the second encryption key supports confidentiality protection of a second security policy between the firewall and the host device. Next, based at least in part upon the second security policy, the first encryption key is requested and the first encryption key is sent under the protection of the second security key and in accordance with the second security policy. Finally, encrypted data is passed when it is determined that the first encryption key is received.